IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CAROL LEE WALKER	:	**CIVIL ACTION**
	:	
v.	:	**NO. 17-40**
	:	
COFFEY, *et al.*	:	
	:	

MEMORANDUM

KEARNEY, J. **April 24, 2017**

We return to the evolving question of an accused employee's Fourth Amendment rights in her emails sent through her employer's servers. When sued for civil rights damages by an exonerated employee now claiming an illegal search and seizure, state prosecutors and investigators seek absolute prosecutorial immunity. We sparingly grant absolute immunity for prosecutorial advocacy in a judicial process. Our decision depends on whether the unique facts evidence prosecutorial conduct which is advocacy or more akin to investigative or police-like evidence gathering activity.

Today we review a facially defective criminal subpoena requiring a university employer to produce its accused employee's emails at an undated time with no location and no scheduled hearing or trial. Based on the unique facts, we find the state prosecutor and investigator are not entitled to absolute immunity as they used this defective subpoena to gather evidence and not for advocacy in a judicial proceeding. But the prosecutor and investigator are entitled to qualified immunity from damages in a civil rights Fourth Amendment illegal search and seizure claim when the accused employee cannot show a clearly established expectation of privacy in her emails stored on her employer's computer after the employer consents.

I. Plead Facts

In July 2015, the Pennsylvania Attorney General filed a criminal complaint against Carol Lee Walker, her husband Ray Allen Walker, Jr., and his trucking company in the Court of Common Pleas of Centre County.[1] The Commonwealth, through Special Deputy Attorney General Brian T. Coffey, charged Ms. Walker with four counts of conspiracy to commit forgery, unlawful use of a computer, unlawful duplication, conspiracy to commit unlawful duplication, conspiracy to commit unlawful use of a computer, and conspiracy to commit unlawful duplication.[2] On August 19, 2015, the Court of Common Pleas conducted a preliminary hearing and held Ms. Walker over on four counts of conspiracy to commit forgery.[3] The court dismissed all other charges against Ms. Walker.

On October 15, 2015, Special Deputy Coffey filed an Information against Ms. Walker with the Court of Common Pleas.[4] In response, Ms. Walker filed a "comprehensive Omnibus Motion for Pretrial Relief attacking the bulk of the remaining charges against [her.]"[5] Ms. Walker alleges the Court of Common Pleas did not schedule a hearing on her Omnibus Pretrial Motion and scheduled her trial date for March 22, 2016.[6]

Ms. Walker alleges Special Deputy Coffey and his investigator, Special Agent Paul Zimmerer, "during a period of prolonged inactivity in the case, hatched a scheme to conduct additional investigation of [Ms.] Walker…by utilizing a fraudulent and illegal subpoena to access the private computer files of [Ms.] Walker."[7]

Ms. Walker alleges Special Deputy Coffey issued an illegal subpoena to her employer Pennsylvania State University.[8] Specifically, Special Deputy Coffey subpoenaed John Corro, Penn State's General Counsel and Senior Security/Systems Analyst.[9] Special Deputy Coffey subpoenaed the production of "any & all emails/compute [sic] files/documents/attachments to or

from Carol Lee Walker, CLW9@psu.edu" followed by several email addresses from 2008 to present.[10] The subpoena does not list a date, time, or place for Mr. Corro to appear and bring the documents with him. Ms. Walker alleges "because the illegal subpoena was in fact being used for investigative activity and not for a proper purpose, it is blank as to the place, date, time and party on behalf of whom testimony is demanded….no hearings or other proceedings were scheduled at the time of the preparation and service of the subpoena."[11]

On October 20, 2015, Judge Thomas K. Kistler of the Court of Common Pleas witnessed the subpoena and the Prothonotary signed it.[12] The next day, October 21, 2015, Special Agent Zimmerer went to Penn State's General Counsel's Office and presented the subpoena to assistant general counsel Katherine Allen.[13] Attorney Allen and her staff agreed to assist Special Agent Zimmerer with the subpoena.[14] Ms. Walker alleges Special Agent Zimmerer returned sometime later and Penn State provided him with her "personal and private email records."[15] Ms. Walker alleges Special Deputy Coffey and Special Agent Zimmerer "knowingly and intentionally used a fraudulent and illegal subpoena in order to obtain access to [Ms.] Walker's private computer records and in fact obtained access to those records."[16]

At some point after this search, the Court of Common Pleas granted the Attorney General's request to *nolle prosequi* with prejudice all charges against Ms. Walker.[17]

II. Analysis

Ms. Walker alleges Special Deputy Coffey and Special Agent Zimmerer violated her Fourth Amendment right by failing to obtain a search warrant to search and seize her personal records.[18] Ms. Walker sues Special Deputy Coffey and Special Agent Zimmerer, in their individual capacities under § 1983, alleging they "acted under the color of state law" when they conducted an illegal search and seizure under the Fourth Amendment.[19] Ms. Walker further

alleges Special Deputy Coffey "encouraged, tolerated, ratified and has been deliberately indifferent to…(a) [Special Agent] Zimmerer's duty to refrain from unlawful and illegal searches and seizures, and (b) [Special Agent] Zimmerer's duty not to use fraudulent and illegal subpoenas."[20] Ms. Walker also alleges Special Deputy Coffey and Special Agent Zimmerer's same actions violated "her right to be free of illegal search and seizure guaranteed by Article I, section 8 of the Pennsylvania Constitution."[21]

Special Deputy Coffey and Special Agent Zimmerer move to dismiss Ms. Walker's § 1983 claim arguing they are entitled to absolute immunity when collecting evidence for trial, or in the alternative, they are entitled to qualified immunity because Ms. Walker does not have a reasonable expectation of privacy in her work email, and even if she did, her right was not clearly established at the time Special Agent Zimmerer served the subpoena.[22] Special Deputy Coffey and Special Agent Zimmerer argue no private right of action exists for her claim under the Pennsylvania Constitution, and even if it does exist, they are protected by sovereign immunity because they serve in the Pennsylvania Office of the Attorney General.

A. Absolute immunity does not apply to this unique conduct.

Special Deputy Coffey and Special Agent Zimmerer argue they are entitled to absolute prosecutorial immunity from Ms. Walker's § 1983 claim. Upon review of the facts, absolute immunity does not apply.

1. Special Deputy Coffey does not enjoy absolute immunity.

Special Deputy Coffey "bears the 'heavy burden' of establishing entitlement to absolute immunity," and because our Supreme Court's "quite sparing" recognition of absolute immunity, we begin by presuming absolute immunity will not apply but qualified immunity may.[23] To overcome our presumption, Special Deputy Coffey "must show he…was functioning as the

state's advocate" when issuing the October 20, 2015 subpoena.[24] "Under this functional approach, [Special Deputy Coffey] enjoys absolute immunity for actions performed in a judicial or 'quasi-judicial' capacity," that is, "actions 'intimately associated with the judicial phases of litigation,' but not to administrative or investigatory actions unrelated to initiating and conducting judicial proceedings."[25] Our Court of Appeals directs us to "focus on the unique facts" and reject "bright-line rules that would treat the timing of the [Special Deputy Coffey]'s action (*e.g.* pre- or postindictment), or its location (*i.e.* in- or out-of-court), as dispositive."[26]

a. Background on absolute prosecutorial immunity.

Special Deputy Coffey's absolute immunity argument is complicated by Ms. Walker's allegation he used a state criminal subpoena as a search warrant to direct a Penn State employee to search and seize Ms. Walker's work emails without probable cause in violation of her Fourth Amendment rights. Ms. Walker's allegation, which we take as true, places Special Deputy Coffey's conduct between two paradigms, a prosecutor's fraudulent conduct in procuring a search warrant and a prosecutor's fraudulent conduct issuing a subpoena to a third-party witness.

As to a search warrant, prosecutors enjoy absolute immunity when filling out a search warrant but not for their accompanying false sworn declaration. In *Kalina v. Fletcher*, a prosecutor filed an information, a motion for an arrest warrant, and "Certification for Determination of Probable Cause" to begin prosecuting the defendant.[27] The prosecutor "personally vouched" for the truth of the Certification, even though it contained two false statements.[28] Based on the prosecutor's sworn false statement, officers arrested and incarcerated the defendant for a day.[29] A month later, the court granted the prosecutor's motion to dismiss charges against the defendant.[30] The defendant then sued the prosecutor and the prosecutor asserted absolute prosecutorial immunity.[31] The Supreme Court held the prosecutor's acts of

"(1) filing the information and (2) filing the motion for an arrest warrant were protected by absolute immunity" because she functioned as an advocate but her act of (3) "personally attesting to the truth of the averment" in the Certification was non-prosecutorial because it could have been performed by any competent witness."[32]

The parties do not cite and we cannot find a factually analogous case as to a prosecutor's absolute immunity when issuing a subpoena *duces tecum* to a defendant's employer for the defendant's emails but inexplicably omitting a date, time, or place for the subpoenaed party to produce the documents. A Court of Appeals case from the Ninth Circuit, *Garmon v. County of Los Angeles*, is similar but not directly on point.[33] The Los Angeles County District Attorney charged the defendant with murder.[34] The defendant wanted his mother to testify as his alibi witness but she had a scheduled brain surgery with uncertain side effects.[35] Instead, the parties took her deposition and she authorized her doctors, Kaiser, to release her medical records regarding her brain tumor to the prosecutor.[36] Instead of receiving the authorized records from Kaiser, the prosecutor issued a subpoena *duces tecum* to the mother's doctors.[37] The prosecutor subpoenaed the mother's entire medical record and in his supporting declaration falsely represented the mother was the murder victim, not a witness.[38] By listing the mother as a murder victim, the prosecutor took advantage of a HIPAA exception which permits Kaiser to disclose a victim's records without consent or notification.[39] The mother did testify at trial, and the prosecutor used the mother's medical history to impeach her testimony during cross-examination.[40] The mother sued numerous parties, including a § 1983 claim against the prosecutor.[41]

The court of appeals began with the premise "issuing a subpoena is necessarily an evidence-gathering action."[42] The court found persuasive the prosecutor issued the subpoena "in

preparation for evaluating and countering" the mother's testimony at trial because she is acting as an advocate.[43] This motivation for the prosecutor's issuance of the subpoena distinguished her performance as "a quasi-judicial advocacy function [where] the prosecutor is 'organiz[ing], evaluat[ing], and marshaling [that] evidence' in preparation for a pending trial, in contrast to the police-like activity of 'acquiring evidence which might be used in a prosecution.'"[44] The court concluded the prosecutor "is entitled to absolute immunity for issuing the subpoena *duces tecum* to Kaiser."[45] The prosecutor was not entitled to absolute immunity for the false statements in her declaration supporting the subpoena.[46] The court of appeals applied *Kalina* to this subpoena and held the prosecutor's declaration is an act "any competent witness might have performed" and the prosecutor made her false statements under "penalty of perjury, making her more akin to a witness than a prosecutor in this function."[47]

b. Special Deputy Coffey's October 20, 2015 subpoena.

Special Deputy Coffey did not function as an advocate when he issued the subpoena *duces tecum* to John Corro. Special Deputy Coffey does not explain why he issued the subpoena; instead he relies on Ms. Walker's allegations. He argues from the Complaint "it is clear" he sought Ms. Walker's "emails in connection with an active prosecution" and "[i]n this context–where charges were pending and a trial was scheduled…[Special Deputy Coffey acted] in [his] capacity as [a] prosecutor."[48]

Special Deputy Coffey cannot meet his "heavy burden" of showing absolute immunity relying solely on the timing of timing of his subpoena during "active prosecution." Our Court of Appeals firmly "reject[s] bright-line rules that would treat the timing of the [Special Deputy Coffey]'s action (*e.g.* pre- or postindictment), or its location (*i.e.* in- or out-of-court), as dispositive."[49] Special Deputy Coffey relies on an incorrect statement of governing precedent

when he suggests our Court of Appeals "draws a distinction between a prosecutor's actions…***prior to*** the filing of a complaint or indictment and ***subsequent to*** such a filing."[50] Our Court of Appeals warned us against this exact temptation "to derive bright-line rules from the [Supreme Court cases]….[but] [t]o preserve the fact-based nature of the inquiry, however, the Supreme Court has cautioned against such categorical reasoning."[51]

First, we perform a "meticulous analysis" of "the nature of the function performed, not the identity of the actor who performed it" to determine if Special Deputy Coffey is entitled to an extraordinary grant of absolute immunity for gathering evidence.[52] Special Deputy Coffey charged Ms. Walker in July 2015. On August 19, 2015, the court conducted a preliminary hearing, held over Ms. Walker on conspiracy charges, and dismissed the remaining charges. On October 15, 2015, Special Deputy Coffey filed an Information against Ms. Walker and a few days later Ms. Walker filed an omnibus pretrial motion. When Special Deputy Coffey issued the subpoena on October 20, 2015, Ms. Walker's motion was pending before the court and the parties had discussed a trial date.[53]

Special Deputy Coffey issued the subpoena lacking a specific date, time, or place for John Corro to appear with the items described. Pennsylvania Rule of Criminal Procedure 107 states "[a] subpoena in a criminal case shall order the witness named to appear before the court at the date, time, and place specified, and to bring any items identified or described."[54] The Comment to Rule 107 explains the use of a criminal subpoena is "not only for trial but also any other stage of the proceedings when a subpoena is issuable, including preliminary hearings, hearings in connection with pretrial and post-trial motions, *etc*."[55]

Special Deputy Coffey's subpoena is deficient under Pennsylvania state law because it lacks a date, time, and place for John Corro to appear. Assuming the court had scheduled Ms.

Walker's trial, Special Deputy Coffey does not explain why he left off the trial date and time from the subpoena, nor does he explain how Ms. Walker's Penn State emails are necessary to his advocacy. Special Deputy Coffey's omission of date and time for a judicial proceeding shows this subpoena for investigation is "unrelated to initiating and conducting judicial proceedings."[56]

In "the gray areas between prosecutorial and investigative activity,"[57] Special Deputy Coffey's subpoena is the "police-like acquiring evidence" for prosecution because there is no judicial proceeding listed and no explanation how this subpoena is necessary for Special Deputy Coffey's advocacy in the unknown judicial proceeding. In *Garmon*, the prosecutor overcame the court of appeals' presumption "issuing a subpoena is necessarily an evidence-gathering action" by showing, based on facts and context, she functioned as an advocate gathering documents to "evaluat[e] and counter[] a defense witness's testimony" at trial.[58] The court of appeals found the most important factor in applying absolute immunity was the prosecutor sought the evidence "in preparation for trial."[59]

Special Deputy Coffey argues absolute immunity applies whenever an attorney issues a subpoena relying on *Koresko v. Solis.*[60] His reliance is misplaced. In *Koresko*, a plaintiff challenged the Department of Labor attorney's issuing of an administrative subpoena for possible ERISA violations.[61] The Department issued the administrative subpoena six years before instituting an ERISA enforcement suit against plaintiff.[62] In a brief analysis, the court concluded absolute prosecutorial immunity applies to the issuance of a subpoena because "it falls within the normal duties of an attorney as he contemplates initiating a case." The holding in *Koresko* does not apply here, first, because a federal agency issuing an administrative subpoena in a non-criminal investigation has no precedential value to a prosecutor issuing a subpoena in a criminal case.[63] Second, *Koresko* applies to an attorney issuing a subpoena before filing an

official investigation, and here, Special Deputy Coffey stresses he already filed criminal charges against Ms. Walker when he issued the subpoena.[64] He faced a possible hearing on Ms. Walker's onmibus motion and, from all plead facts, sought to investigate further facts.

At the time Special Deputy Coffey issued the subpoena, he functioned as an investigator and not as an advocate preparing for a judicial proceeding identified on the subpoena. Special Deputy Coffey's reliance on the existence of "active prosecution" because the court held Ms. Walker over on conspiracy charges after a preliminary hearing and may have scheduled a trial date five months out is not enough to overcome the presumption of qualified immunity. In *Garmon,* the court of appeals found a clear advocacy function for the prosecutor's subpoena, a specific witness and specific need for the documents for the witness to find absolute immunity.[65]

We deny absolute prosecutorial immunity because, after our "meticulous analysis" of the facts, Special Deputy Coffey does not meet his "heavy burden" to show how he functioned in a quasi-judicial advocate for the Commonwealth when he signed this subpoena not tied to any judicial proceeding sent to a witness not being ordered to testify.[66] Special Deputy Coffey investigated potentially new sources of information when issuing the facially invalid subpoena. While always an attorney, the unique circumstances of this conduct evidence an investigative intent. He did not request testimony. He did not compel a witness to appear at a judicial proceeding. He wanted data from a computer server. Had he tied this subpoena unmoored to any ongoing litigation to an advocacy role in some judicial proceeding, he would have a stronger argument as to absolute prosecutorial immunity. We have no basis to tie this invalid subpoena to initiating or conducting legal proceedings.

2. Special Agent Zimmerer is not entitled to absolute immunity.

Special Agent Zimmerer's claim of absolute prosecutorial immunity is derivative of Special Deputy Coffey's immunity.[67] As we find no basis to grant absolute prosecutorial immunity to Special Deputy Coffey, we similarly deny absolute prosecutorial immunity for Special Agent Zimmerer.

B. The prosecutor and investigator are entitled to qualified immunity.

Special Deputy Coffey and Special Agent Zimmerer also argue qualified immunity bars damages recovery on Ms. Walker's claims because their search did not violate Ms. Walker's federal rights, and in the alternative, Ms. Walker's reasonable expectation of privacy in her work emails was not clearly established at the time. Ms. Walker argues qualified immunity does not apply because Special Deputy Coffey and Special Agent Zimmerer "(1) violated her civil rights; and, (2) "the right in question was clearly established at the time of the violation."[68]

The Supreme Court "stress[es] the importance of resolving immunity questions at the earliest possible stage in litigation."[69] We use our discretion to decide which qualified immunity prong to address first "in light of the circumstances in the particular case at hand."[70] We proceed to the clearly established prong when "it is plain that a constitutional right is not clearly established but far from obvious whether in fact there is such a right."[71] Ms. Walker's objectively reasonable expectation of privacy in her work emails is a complicated fact intensive inquiry requiring discovery and depositions but whether her right is clearly established is plain.[72]

Ms. Walker cannot show a clearly established right. Accepting as true Ms. Walker's allegation Penn State functioned as her Internet Service Provider and the Stored Communications Act applied, there is "neither Supreme Court precedent nor a 'robust consensus of cases of

persuasive authority'" establishing an expectation of privacy in email communications under the Fourth Amendment.[73]

Ms. Walker argues the Federal Stored Communications Act established her constitutional violation and the need for Special Deputy Coffey and Special Agent Zimmerer to acquire a warrant by calling Penn State her "internet service provider." Ms. Walker cites to 18 U.S.C. § 2703(b) as establishing the need for a warrant, however, the title of §2703 is "Required disclosure of ***customer*** communications or records."[74]

Ms. Walker directs us to *United States v. Warshak* for the proposition she has a clearly established expectation of privacy in her emails held by Penn State, her internet service provider.[75] We do not agree *Warshak* establishes a clear right, particularly in light of the opinion's narrow holding and conflicting case law. In *Warshak*, the federal government investigated defendant and his company for fraud.[76] Defendant and his company had an email account with NuVox, an internet service provider.[77] In October 2004, the government requested NuVox preserve defendant's emails sent to and from his NuVox account under § 2703(f) of the Stored Communication Act.[78] Per the government's request, NuVox preserved copies of defendant's emails without defendant's knowledge over the next four months.[79] In January 2005, the government subpoenaed NuVox to turn over the preserved emails and in May 2005, the court issued an *ex parte* order for Nuvox to turn over defendant's remaining emails to the government.[80] The defendant did not receive notice NuVox preserved and turned over approximately 27,000 emails to the government until May 2006.[81] Defendant moved to suppress the emails because the government's warrantless search violated the Fourth Amendment.

The court of appeals found emails are analogous to letters and phones and the internet service provider "is the functional equivalent to a post office or a telephone company."[82] If

emails have the same protection as calls and letters, "it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment."[83] The court of appeals, however, tempered its holding in two ways. First, the court is "unwilling" to find an email subscriber and an internet service provider could never enter into an agreement which "extinguish[es] a reasonable expectation of privacy."[84] The court also recognized its holding "may be attacked in light of the Supreme Court's decision in *United States v. Miller*" where the Supreme Court held "a bank depositor does not have a reasonable expectation of privacy in the contents of bank records, checks, and deposits slips."[85] The court briefly distinguished *Miller* because an internet service provider is an intermediary, where a bank is the intended recipient of the documents.[86]

Since *Warshak* in 2010, "neither Supreme Court precedent nor a 'robust consensus of cases of persuasive authority'" as required by our Court of Appeals establish an employee's expectation of privacy in email communications on her employer's server under the Fourth Amendment.[87] A district court commented, "[a]lthough the Sixth Circuit declared the existence of that right in 2010…the continued validity of the Stored Communications Act and ever-developing law governing access to electronic communications around the country negates a conclusion that the Sixth Circuit's holding alone made an individual's expectation of privacy in his or her emails clearly established through the country as of 2012."[88]

Ms. Walker argues *Warshak* established "an unquestioned principle of law that email communications have a reasonable expectation of privacy," however, her supporting caselaw does not support her proposition. Ms. Walker cites to a concurring opinion in *United States v. Davis* as support but the majority opinion contradicts Ms. Walker's reliance.[89] In *Davis*, the government requested the defendant's telephone records from his cellular service provider under

the Stored Communications Act.[90] The cellular service provider produced "to and from" and times of defendant's calls but not the content or location of calls/texts.[91] The defendant moved to suppress arguing the cellular service provider's actions constituted a search under the Fourth Amendment so the government needed a search warrant.[92] The district court denied the motion.[93] In the majority precedential opinion, the Court of Appeals for the Eleventh Circuit held defendant had no subjective or objective reasonable expectation of privacy in the call records stored by his cellular service provider.[94] The majority opinion relies heavily on *United States v. Miller*, the case which the Court of Appeals for the Sixth Circuit distinguished from in *Warshak* showing this right is far from clearly established in the courts of appeal.

Ms. Walker argues other courts have relied on *Warshak* as clearly establishing a right to privacy in her email communications. Ms. Walker's argument is not persuasive and her reliance is misplaced. In *Vista Marketing, LLC v. Burkett*, an ex-wife accessed her ex-husband's work email during their divorce proceedings and the husband's employer brought a claim under the Stored Communications Act.[95] It has no precedential value because it involves no Fourth Amendment claim and no government actors. In *United States v. Graham*, the court held the government did not need a warrant to obtain defendant's historical cell location data from his cellular service provider under the Stored Communications Act.[96] *Warshak* is only mentioned in the court's summation of the defendant's argument he has the same privacy interest in his historical location data as he may have in the content of emails.[97] Ms. Walker's cite to our Court of Appeals' decision in *Schuchardt v. United States* is equally unavailing.[98] In *Schuchardt*, the plaintiff challenged the government's surveillance under § 702 of the Foreign Intelligence Surveillance Act.[99] The court cites *Warshak* when addressing whether plaintiff has an individualized grievance for standing to sue and for the proposition plaintiff's privacy right is

"neither indivisibly abstract nor indefinite."[100] *Schuchardt* does not involve a criminal investigation or the Stored Communications Act and does not clearly establish an employee's constitutionally protected expectation of privacy in emails when the employer consents.

Ms. Walker's failure to show *Warshak* clearly established a right to privacy in her emails becomes murkier because while Ms. Walker alleges Penn State is her internet service provider, Penn State is also her employer and provides Ms. Walker with the @psu.edu email address. It is not clear *Warshak*'s holding regarding "commercial" internet service provider under the Stored Communications Act extends into the employment context. The title of §2703 is "Required disclosure of ***customer*** communications or records."[101] The year before *Warshak*, a district court within the Sixth Circuit faced a similar search by an employer.[102] In *United States v. Hart*, the defendant moved to suppress email his employer found on defendant's private email accessed on his work computer.[103] The defendant alleged the Stored Communications Act governed his employer's search of his work computer.[104] The court disagreed. It noted even though defendant's employer "is, in fact, an internet service provider" to customers, there is no evidence defendant is a customer. "Rather, he was [an] employee, who was permitted by his employer to use its internet service…to send and receive emails."[105]

The distinction between a customer using a commercial internet service provider and an employee using internet provided by her employer is crucial because we find no controlling precedent and it is not clearly established a law enforcement agent needs a search warrant to seize an employee's email/computer files when the employer consents. In *United States v. Yudong Zhu*, the defendant, an assistant professor at New York University, acquired a laptop with government funds.[106] The university employer owned the laptop but the defendant took it home with him every night, encrypted the hard drive, and added passwords.[107] Defendant signed

the university employer's computer policy allowing it the right to inspect his laptop without notice.[108] The university employer began investigating the defendant for honest services fraud.[109] The defendant turned his laptop over to his employer but refused to give his passwords.[110] The employer university contacted the FBI and turned the defendant's laptop over to them without the defendant's consent.[111] The FBI decrypted and searched the defendant's laptop without obtaining a search warrant.[112] The United States later charged the defendant and the defendant moved to suppress the FBI's findings from the laptop search arguing the search violated his Fourth Amendment rights because they did not have a warrant.[113] While the defendant "had a reasonable expectation of privacy in relation to the FBI's search of his laptop, the Court is persuaded that the search here was performed with NYU's valid, third-party consent."[114] The university employer could consent to the FBI search because it had access to the laptop through defendant's consent to allow the employer to inspect it.[115] The university employer also "exercised common authority over the laptop, it has a substantial interest in the laptop, and it had permission to access the laptop."[116]

Ms. Walker alternatively argues she has a clearly established right to the privacy of her employee emails when requested by a facially invalid subpoena. She provides no caselaw suggesting the invalidity of the underlying subpoena under state law is a factor leading to a clearly established right precluding the production of information otherwise available with the employer's consent. We are guided by a 2007 decision by a court of appeals holding law enforcement agents do not need a warrant to search an employee's work computer when the employer consents to the search.[117] Under *Ziegler* and *Yudong Zhu*, it is plain a constitutional right to require law enforcement agents to have a warrant before they search an employee's work computer/emails is not clearly established because both courts state an employer can consent to

the warrantless search.[118] If law enforcement does not need a search warrant to search an employee's work computer when the employer consents, and absent any clearly established law, we cannot find a procedurally defective subpoena somehow falls within a clearly established right.

Ms. Walker alleges Special Agent Zimmerer went to Penn State with a deficient subpoena to acquire emails, files, documents, and attachments from her Penn State provided email (@psu.edu) to 7 email addresses.[119] While Ms. Walker alleges Special Deputy Coffey and Special Agent Zimmerer subpoenaed Penn State "in its capacity as an Internet Service Provider," Ms. Walker cannot artfully plead around the fact her @psu.edu email is provided by her employer, Penn State.[120] Unlike *Yudong Zhu*, where the defendant gave his employer consent to inspect his laptop, Ms. Walker does not allege she gave Penn State permission to search her work email. Ms. Walker, however, produced no case law holding an employer must have an employee's signed consent before allowing a search of its own email servers relating to its employee's accounts. We do not opine, or suggest in any way, our present holding applies to student or non-employee emails which may, under the Stored Communications Act, allow a consumer certain protections. We also do opine on whether this information would have been suppressed under Pennsylvania criminal law.

Ms. Walker also attaches Special Agent Zimmerer's Investigative Report noting Penn State assisted with the subpoena and alleges Penn State conducted the search itself and Special Agent Zimmerer "picked up the records from Penn State."[121] We find these notes support qualified immunity as they further evidence the employer's consent. We are also not aware of any clearly established law limiting the state prosecutors to using warrants rather than subpoenas to gather evidence. Ms. Walker has no clearly established constitutional right because no court

has required law enforcement agents to obtain a warrant to search an employee's computer files/emails where the employer provides the computer and consents to the search.[122] Special Deputy Coffey and Special Agent Zimmerer are entitled to qualified immunity because Ms. Walker has no clearly established constitutional right when no controlling precedent required law enforcement agents to obtain a warrant to search an employee's computer files/emails where the employer provides the computer and consents to the search.[123]

C. Ms. Walker cannot plead Pennsylvania Constitution claims.

Ms. Walker's claims under the Pennsylvania Constitution are dismissed. "No Pennsylvania statute establishes, and no Pennsylvania court has recognized, a private cause of action for damages under the Pennsylvania Constitution."[124]

III. Conclusion

Absolute prosecutorial immunity does not apply to Special Deputy Coffey and Special Agent Zimmerer's unique investigative conduct through a facially invalid subpoena. But qualified immunity bars Ms. Walker's suit because Ms. Walker's constitutional right in the privacy of her employment emails when an employer consents in response to a criminal subpoena was not clearly established at the time the state actors subpoenaed her university employer to search her work email and files. We also dismiss Ms. Walker's claims under the Pennsylvania Constitution because she cannot bring a private cause of action for damages under Art.1 § 8 of the Pennsylvania Constitution.

---

[1] ECF Doc. No. 5 ¶ 15.

[2] *Id.*

[3] *Id.* ¶ 19.

[4] *Id.* ¶ 20.

[5] *Id.*

[6] *Id.*

[7] *Id.* ¶ 21.

[8] *Id.* ¶ 24.

[9] *Id.*

[10] *Id.* ¶ 27.

[11] *Id.* ¶ 26.

[12] *Id.* at Exhibit B.

[13] ECF Doc. No. 5 ¶ 22.

[14] *Id.*

[15] *Id.* ¶ 33.

[16] *Id.* ¶ 31.

[17] *Id.* ¶ 40.

[18] *Id.* ¶¶ 35-36.

[19] *Id.* ¶ 43.

[20] *Id.* ¶ 44.

[21] *Id.* ¶ 48-51.

[22] "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim satisfies the plausibility standard when the facts alleged "allow[] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Burtch v. Millberg Factors, Inc.*, 662 F.3d 212, 220-21 (3d Cir. 2011) (citing *Iqbal*, 556 U.S. at 678). While the plausibility standard is not "akin to a 'probability requirement,'" there nevertheless must be more than a "sheer possibility that a defendant has acted unlawfully." *Iqbal*, 556 U.S. at 678 (citing *Twombly*, 550

U.S. at 556). "Where a complaint pleads facts that are 'merely consistent with' a defendant's liability, it 'stops short of the line between possibility and plausibility of entitlement to relief.'" *Id.* (quoting *Twombly*, 550 U.S. at 557).

The Court of Appeals requires us to apply a three-step analysis under a 12(b)(6) motion: (1) "it must 'tak[e] note of the elements [the] plaintiff must plead to state a claim;'" (2) "it should identify allegations that, 'because they are no more than conclusions, are not entitled to the assumption of truth;'" and, (3) "[w]hen there are well-pleaded factual allegations, [the] court should assume their veracity and then determine whether they plausibly give rise to an entitlement for relief." *Connelly v. Lane Construction Corp.*, 809 F.3d 780, 787 (3d Cir. 2016) (quoting *Iqbal*, 556 U.S. at 675, 679); *see also Burtch*, 662 F.3d at 221; *Malleus v. George*, 641 F.3d 560, 563 (3d. Cir. 2011); *Santiago v. Warminster Township*, 629 F.3d 121, 130 (3d. Cir. 2010).

[23] *Odd v. Malone*, 538 F.3d 202, 207-8 (3d Cir. 2008) (quoting *Light v. Haws*, 472 F.3d 74, 80–81 (3d Cir.2007) (internal citation omitted) and *Carter v. City of Philadelphia*, 181 F.3d 339, 335 (3d Cir. 1999)).

[24] *Id.* at 208 (*Yarris v. County of Delaware*, 465 F.3d 129, 134 (3d Cir. 2006)).

[25] *Id.* (quoting *Giuffre v. Bissell*, 31 F.3d 1241, 1251 (3d Cir. 1994)(citing *Imbler v. Pachtman*, 424 U.S. 409, 430 (1976))).

[26] *Id.* at 210 (citing *Yarris*, 465 F.3d at 136; *Kulwicki v. Dawson*, 969 F.2d 1454, 1459 (3d Cir. 1992); and *Rose v. Bartle*, 871 F.2d 331, 346 (3d Cir. 1989)).

[27] *Kalina v. Fletcher*, 522 U.S. 118, 120 (1997).

[28] *Id.* at 121.

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *Odd*, 538 F.3d at 210 (citing *Kalina*, 522 U.S. at 502).

[33] *Garmon v. County of Los Angeles*, 828 F.3d 837 (9th Cir. 2016).

[34] *Id.* at 841.

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] *Id.* at 844 (internal citations omitted).

[45] *Id.*

[46] *Id.* at 844.

[47] *Id.* at 845 (quoting *Kalina*, 522 U.S. at 129-130).

[48] ECF Doc. No. 8 at 5.

[49] *Odd*, 538 F.3d at 210 (citing *Yarris*, 465 F.3d at 136; *Kulwicki*, 969 F.2d at 1459; and *Rose*, 871 F.2d at 346).

[50] ECF Doc. No. 8 at 4 (emphasis added by Defendants).

[51] *Odd*, 538 F.3d at 210 (internal citations omitted).

[52] *Id.* at 208 (quoting *Light*, 472 F.3d at 78-79).

[53] In her Complaint, Ms. Walker alleges the court scheduled her trial for March 22, 2016. In her brief, Ms. Walker now alleges trial was not scheduled when Special Deputy Coffey issued the subpoena and offers to amend her complaint. ECF Doc. No. 5 at 16.

[54] Pa. R. Crim. P. 107.

[55] Pa. R. Crim. P. 107, Comment (2017).

[56] *Odd*, 538 F.3d at 208. (quoting *Giuffre*, 31 F.3d at 1251)(citing *Imbler*, 424 U.S. at 430)).

[57] *Light*, 472 F.3d at 80 (quoting *Schrob v. Catterson*, 948 F.2d 1402, 1414 (3d Cir. 2007)).

[58] *Garmon*, 828 F.3d at 844.

[59] *Id.*

[60] *Koresko v. Solis*, No. 09-3152, 2011 WL 557435 (E.D. Pa. Nov. 10, 2011).

[61] *Id.* at *1.

[62] *Id.* at *3.

[63] *See id*.

[64] *See id*.

[65] *See Garmon*, 828 F.3d at 844.

[66] *See Odd*, 538 F.3d at 208.

[67] *See Moore v. Middlesex Cty. Prosecutors Office*, 503 Fed. Appx. 108, 109 (3d Cir. 2012)(citing *Davis v. Grusemeyer*, 996 F.2d 617, 631 (3d Cir. 1993) *overruled on other grounds by Rolo v. City Investing Co. Liquidating Trust*, 155 F.3d 644 (3d Cir.1998)) ("This Court has held, for example, that absolute immunity extends to employees of prosecutors who perform investigative work in furtherance of a criminal prosecution").

[68] *Schneyder v. Smith*, 653 F.3d 313, 319 (3d Cir. 2011).

[69] *Pearson v. Callahan*, 555 U.S. 223, 232 (2009) (quoting *Hunter v. Bryant*, 502 U.S. 224, 227 (1991)).

[70] *Id.* at 236.

[71] *Id.* at 237.

[72] *United States v. Nagle*, 803 F.3d 167, 176 (3d Cir. 2015) (quoting *United States v. Donahue*, 764 F.3d 293, 298-99 (3d Cir. 2014)) (To prove a legitimate expectation of privacy, Ms. Walker must show (1) "an actual or subjective expectation of privacy in the subject of the search or seizure"; and, (2) her "expectation of privacy is objectively justifiable under the circumstances").

[73] *Mirabella v. Villard*, --- F.3d ---, 2017 WL 1228552 at *18 (3d Cir. 2017).

[74] 18 U.S.C. § 2703 (emphasis added).

[75] At oral argument, Ms. Walker's counsel asked for leave to file a supplemental memorandum supplying caselaw showing Ms. Walker's right is clearly established. Ms. Walker's supplemental memorandum did not identify new persuasive authority. Both parties discuss the Supreme Court's analysis in *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010); it does not

govern for two reasons. First, in *Quon*, the Supreme Court assumed for the purposes of argument, but did not decide, the employee had an objectively reasonable expectation of privacy in his employer provider pager. The court also assumed the government employer's reading of employee's text messages is a search under the Fourth Amendment. *Id.* The only precedential holding in *Quon* is the reasonableness of the government employer's search. *Id.* at 761. Second, *Quon* is not a criminal investigation. *Quon* deals with the expectation of privacy between an employee and employer when the employer is a government entity. Ms. Walker's claim is different; it deals her reasonable expectation of privacy in her work email from a government's agent criminal investigation where her employer consents to the search.

[76] *United States v. Warshak*, 631 F.3d 266, 281 (6th Cir. 2010).

[77] *Id.* at 283.

[78] *Id.*

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *Id.* at 286.

[83] *Id.*

[84] *Id.*

[85] *Id.* at 288 (citing *United States v. Miller*, 425 U.S. 435, 442 (1976)).

[86] *Id.*

[87] *Mirabella*, 2017 WL 1228552 at *187.

[88] *Kelley v. Fed. Bureau of Investigation*, 67 F. Supp. 3d 240, 272 n. 22 (D.D.C. 2014) (internal citations omitted).

[89] *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (en banc).

[90] *Id.* at 502.

[91] *Id.*

[92] *Id.* at 503.

[93] *Id.*

[94] *Id.* at 511.

[95] *Vista Marketing, LLC v. Burkett*, 812 F.3d 954 (11th Cir. 2016).

[96] *United States v. Graham*, 824 F.3d 421, 427 (4th Cir. 2016) (en banc).

[97] *Id.* at 433.

[98] *Schuchardt v. United States*, 839 F.3d 336 (3rd Cir. 2016).

[99] *Id.* at 338.

[100] *Id.* at 346.

[101] 18 U.S.C. § 2703 (emphasis added).

[102] *United States v. Hart*, No. 08-109, 2009 WL 2552347 (W.D. Ky. Aug. 17, 2009).

[103] *Id.* at *19.

[104] *Id.*

[105] *Id.*

[106] *United States v. Yudong Zhu*, 23 F. Supp. 3d 234, 236 (S.D.N.Y. 2014).

[107] *Id.*

[108] *Id.* at 240.

[109] *Id.* at 236.

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] *Id.* at 240 (the court looked to *Mancusi v. DeForte*, 392 U.S. 364, 365 (1968) where the Supreme Court "acknowledged that an employee may have different expectations of privacy regarding a search by an employer versus a search by the government").

[115] *Id.*

[116] *Id.* at 241.

[117] *See United States v. Ziegler*, 474 F.3d 1184, 1192 (9th Cir. 2007) (although defendant had a reasonable expectation of privacy in his office, "Frontline, as the employer, could consent to a [FBI] search of the office and the computer that it provided to [defendant] for his work").

[118] *See id.*;*Yudong Zhu*, 23 F. Supp. 3d at 240.

[119] ECF Doc. No. 5 ¶ 27.

[120] *Id.* ¶ 3.

[121] *Id.* ¶ 33, at 14.

[122] *See Yudong Zhu*, 23 F. Supp. 3d at 236.

[123] *See id*.

[124] *Pocono Mountain Charter School v. Pocono Mountain School District*, 442 Fed. Appx. 681, 687 (3d Cir. 2011) (citing *Moeller v. Bradford County*, 444 F. Supp. 2d 316, 320-21 (M.D. Pa. 2006)).